IN THE CLAIMS

1 (Currently Amended). An apparatus, comprising:

a detector to determine whether a first radio frequency identification tag read by a reader that reads radio frequency identification tags is a match with a second radio frequency identification tag read by said reader[[.]] and

wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector includes a nonce generator to generate a nonce, and a comparator to compare an encrypted version of the nonce encrypted using a cryptography key of the lock tag with an encrypted version of the nonce encrypted using a cryptography key of the key tag.

2 (Original). An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag.

3 (Original). An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector authenticates the lock tag when said detector detects the lock tag and the key tag being within a predetermined distance of said detector.

4 (Currently Amended). An apparatus as claimed in 1, ~~wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector includes a nonce generator to generate a nonce,~~ including an encryptor to encrypt a nonce using a public cryptography key received from the lock tag to provide an encrypted nonce to the key tag, and a comparator to compare a nonce generated by the nonce generator with a decrypted version of the encrypted nonce that was decrypted using a private cryptography key of the key tag.

Claim 5 (Canceled).

6 (Currently Amended). An apparatus as claimed in claim [[5]] 1, wherein the cryptography key of the lock tag is the same as the cryptography key of the key tag.

7 (Currently Amended). An apparatus as claimed in claim [[5]] 1, wherein the nonce generator generates a series of nonces, wherein the lock tag delays encryption of the nonce with respect to encryption of the nonce by the key tag, and wherein said detector further comprises a delay to delay the encrypted version of the nonce encrypted by the key tag.

8 (Original). An apparatus as claimed in claim 1, wherein said detector determines whether the first radio frequency identification tag is a match with the second radio frequency identification tag or a third or more radio frequency identification tags.

Claims 9-13 (Canceled).

14 (Previously Presented). A method, comprising:

generating a nonce;

encrypting the nonce using a cryptography key received from a first radio frequency identification tag to result in an encrypted nonce;

sending the encrypted nonce to a second radio frequency identification tag that decrypts the encrypted nonce to result in a decrypted nonce;

receiving the nonce from the second radio frequency identification tag;

comparing the nonce generated by said generating to the decrypted nonce; and

determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

Claim 15 (Canceled).

16 (Original). A method as claimed in claim 14, wherein the cryptography key received from the first radio frequency identification tag is a public key, and wherein the second radio frequency identification tag decrypts the encrypted nonce using a private key associated with the public key.

17 (Previously Presented). A method, comprising:

generating a series of nonces;

sending the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag;

receiving encrypted versions of the series of nonces from the first and second radio frequency identification tags;

comparing the encrypted versions of the series of nonces received from the first radio frequency identification tag with the encrypted versions of the series of nonces received from the second radio frequency identification tag; and

determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

Claim 18 (Canceled).

19 (Original). A method as claimed in claim 17, wherein the first and second radio frequency identification tags encrypt the series of nonces using the same cryptography key.

20 (Original). A method as claimed in claim 17, wherein the first radio frequency radio identification tag delays the series of nonces with respect to the second radio frequency identification tag, and further comprising delaying the encrypted versions of the series of nonces received from the second radio frequency identification tag prior to said comparing.

Claims 21-25 (Canceled).

26 (Previously Presented). An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a nonce;

encrypting the nonce using a cryptography key received from a first radio frequency identification tag to result in an encrypted nonce;

sending the encrypted nonce to a second radio frequency identification tag that decrypts the encrypted nonce to result in a decrypted nonce;

receiving the nonce from the second radio frequency identification tag;

comparing the nonce generated by said generating to the decrypted nonce; and

determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

Claim 27 (Canceled).

28 (Original). An article as claimed in claim 26, wherein the cryptography key received from the first radio frequency identification tag is a public key, and wherein the second radio frequency identification tag decrypts the encrypted nonce using a private key associated with the public key.

29 (Previously Presented). An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a series of nonces;

sending the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag;

receiving encrypted versions of the series of nonces from the first and second radio frequency identification tags;

comparing the encrypted versions of the series of nonces received from the first radio frequency identification tag with the encrypted versions of the series of nonces received from the second radio frequency identification tag; and

determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

Claim 30 (Canceled).

31 (Original). An article as claimed in claim 29, wherein the first and second radio frequency identification tags encrypt the series of nonces using the same cryptography key.

32 (Original). An article as claimed in claim 29, wherein the first radio frequency radio identification tag delays the series of nonces with respect to the second radio frequency identification tag, and wherein the instructions, when executed, further result in verification of association of at least two or more radio frequency identification tags by comprising delaying the encrypted versions of the series of nonces received from the second radio frequency identification tag prior to said comparing.

Claims 33-36 (Canceled).